

Users, roles and permissions

DOCUMENT	VERSION	STATUS
SB-GD-103	1.0, October 2026	Public. Checked against the product, October 2026

Who this is for

Owners and Admins who manage who can sign in to SynapBridge and what each person can do.

Before you start

- You need the Owner or Admin role to open the Admin center.
- Roles apply to the whole tenant. There are no roles that apply to one workspace only, and workspaces have no member lists.
- Find the pages in this guide under Admin center: Users, Groups and Roles. Owners and Admins also reach Users from the account menu.

Roles

Built-in roles

- **Owner:** the highest role. Only an Owner can grant the Owner role. Only an Owner can open the billing portal, which changes the payment method and plan and cancels the subscription. The Identity provider (single sign-on), SCIM provisioning and SIEM streaming pages are Owner-only. The pricing page lists all three under the Business plan.
- **Admin:** opens the Admin center and manages users and settings. An Admin can grant only Member and Viewer. An Admin can approve policies, read the audit trail and export it, subject to plan.
- **Member:** standard access. In the plan-gated governance features, a Member can write (for example create and edit policies, router rules and use cases) but cannot approve.
- **Viewer:** read-only. A Viewer appears in the read lists of governance features and in none of the write lists.

Governance roles

An Owner or Admin can give a user one of these roles after the user has joined. They cannot be set in the invite. A person has one role, so choosing a governance role replaces their Member or Viewer role.

- Compliance Officer: allowed by the compliance graph services.
- Security Analyst: allowed to triage shadow AI detections.
- Auditor and External Auditor: allowed to search the audit log through the audit search service.
- Support Admin: recognised by the platform. Check what it can reach in your tenant before you assign it.

To set one, open Admin center, then Users, open the user, choose "Edit", pick the role under "Governance roles", and choose "Save changes".

Note The Admin center pages open only for Owners and Admins, and the sidebar Governance item is shown to Owners and Admins. Test what a person with a governance role can open in your tenant before you rely on that role for an audit.

Custom roles

Custom roles are for per-surface permissions beyond the built-in roles. The pricing page lists them under the Business plan. They can show as off for a workspace.

- 1 Open Admin center, then Roles, then "Custom roles". Built-in roles are listed as Built-in and are read-only.
- 2 Choose "Create role".
- 3 Enter a role name of 1 to 64 characters. The name cannot be changed later, and it cannot match a built-in role name. Add a description if you like.
- 4 In the permissions matrix, tick the actions you want on each surface. Actions marked "reserved" belong to the Owner role and cannot be given to a custom role.
- 5 Choose "Create role".
- 6 To give the role to people, choose "Assign" on the role and pick users.

Related pages under Roles: "Segregation of duties" holds rules that stop one person acting on both sides of a high-stakes workflow, and a rule can block a role change. "Delegated admin" holds scoped admin grants. "Assignments" lists who has which role and whether it came directly, from a group, or from a single sign-on claim.

Deleting a custom role removes its permissions from every user who had it.

Plan-gated permissions

These come from the entitlement matrix. Both the plan and the role must allow an action.

- Read the audit log: Pro plan or above. Owner and Admin.
- Export the audit log: Business or above. Owner and Admin.
- Read policies: Business or above. Owner, Admin, Member, Viewer.
- Write policies: Business or above. Owner, Admin, Member.
- Approve policies: Business or above. Owner and Admin.
- Compliance report download: Business or above. Owner, Admin, Member.
- Kill switch (request and approve), policy rollout and compliance report generation: Enterprise. Owner and Admin.

Invite people

- 1 Open Admin center, then Users, then "Add user".
- 2 Enter the email. Pick Viewer, Member or Admin. Owners can invite as Admin. Admins can invite as Member or Viewer.
- 3 Choose "Send invite".
- 4 The person gets an email with a link that expires in 7 days. They choose a password of at least 12 characters and set up MFA.
- 5 To invite many people, use "Bulk import" on the Users page (up to 512 KiB and 1000 rows). If the page says it is not available for your workspace yet, invite people one at a time.
- 6 To resend an invite, send it again for the same email. A new link replaces the old one. If the person already accepted, nothing is sent.

Outside partners can be added as guests under Users, then "Guest users". Guests get a magic-link email, see only the groups you scope them to, and always expire on a date you set (no more than 365 days ahead).

Change a role

- 1 Open Admin center, then Users, open the user, and choose "Edit". Or select users on the list and use "Change role".
- 2 Pick the new role and save.
- 3 The person sees "Your role changed" and chooses "Refresh session" so every page sees the change.

An Owner can grant any of Owner, Admin, Member and Viewer. An Admin can grant Member and Viewer. The user service also applies a last-Owner guard, role-elevation checks and a block on editing your own account. Segregation-of-duties rules are checked against role changes.

Remove or pause a person

- Suspend: the person is signed out and cannot sign back in until you choose "Reactivate".
- Delete: removes the person's account and their place in the workspace, and you cannot undo it from the Users page. The confirmation says data they owned is kept under your retention policy. If you may want the person back, suspend instead. You cannot delete yourself or the last Owner. Deletions show up in the audit trail under "User deletions".
- Revoke sessions: on the user page, open the Sessions tab and choose "Revoke all sessions".
- Reset password sends a reset email and signs the person out. Reset MFA clears their authenticator secret, asks them to enrol again at next sign-in, and invalidates their recovery codes.

Groups

Open Admin center, then Groups, then "Create group". Security groups can hold role assignments, and every member inherits them. Distribution groups are for addressing only. Deleting a group removes the roles it granted but keeps its members.

Limits and notes

- There is no Tenant Admin or Workspace Admin role.
- Changing a role does not take effect in an open session until the session is refreshed.
- SSO and SCIM are Owner-only pages and are listed under the Business plan.
- Groups, custom roles and some admin pages can show "not available for your workspace yet". Contact support to enable them.
- Some actions ask for your admin password before they run.
- Whether a Viewer can send chat messages is not set by the entitlement matrix. Test with a Viewer account.
- SynapBridge is architected to align with the SOC 2 Trust Services Criteria. Do not put protected health information into SynapBridge until a signed HIPAA agreement exists. That program is planned.